всех проявлений идеологии терроризма в информационно-телекоммуникационных сетях на межгосударственном и национальном уровнях, включая отслеживание устремления зарубежных и внутренних экстремистских, радикальных националистических и террористических организаций.

Список основных источников

1. Авалян, Р. А. Противодействие идеологии экстремизма и терроризма в молодежной среде / Р. А. Авалян // Ростовский научный журнал. — 2017. — № 2. — С. 18–26.

2. Токманцев, Д.В. Меры уголовно-правового предупреждения терроризма и экстремизма / Д. В. Токманцев // Современные системы безопасности — Антитеррор : материалы конгрессной части X специализированного форума, 28–29 мая 2014 г. — Красноярск, 2014. — С. 122–126.

УДК 343.9

Д. Л. Харевич

доцент кафедры оперативно-розыскной деятельности факультета милиции Академии МВД Республики Беларусь, кандидат юридических наук, доцент

О ПЕРСПЕКТИВАХ СОВЕРШЕНСТВОВАНИЯ ПРАВОВОГО ОБЕСПЕЧЕНИЯ БОРЬБЫ СО СБЫТОМ НАРКОТИКОВ В СЕТИ ИНТЕРНЕТ

В последние годы особую актуальность для правоохранительных органов Республики Беларусь приобрела борьба со сбытом наркотиков, совершаемым с использованием возможностей сети Интернет. Данный способ наркосбыта явился серьезным вызовом правоохранительным органам, что потребовало выработки новых подходов в тактике противодействия высокотехнологичной наркопреступности. На решение данной проблемы были направлены усилия представителей белорусской школы оперативно-розыскной деятельности, в трудах которых сделано обобщение выработанных оперативно-розыскной практикой тактических приемов выявления и идентификации наркопреступников, совершающих преступления в сети Интернет. Вместе с тем необходимо отметить, что эффек-

тивность применения таких тактических приемов в значительной степени зависит от особенностей ведения преступной деятельности, способов совершения преступлений и уклонения от привлечения к ответственности. Постоянное совершенствование преступниками этих особенностей и способов усложняет или может сделать невозможным их изобличение с использованием ранее апробированных оперативными сотрудниками приемов, что требует изменения тактики противодействия таким преступлениям.

Изучая зарубежный опыт борьбы с рассматриваемыми преступлениями, можно отметить, что наиболее часто используемые на постсоветском пространстве способы совершения рассматриваемых преступлений отличаются от таковых в других странах мира. Например, интернет-магазины белорусских наркодилеров часто располагаются в открытом сегменте сети Интернет, в то время как за рубежом во многих случаях для этого используется теневой сегмент Интернета, предоставляющий его пользователям более высокую степень анонимности и услуги по принципу «все включено», например, не требуя и даже ограничивая использование сторонних сервисов, мессенджеров, действующих в открытом сегменте Сети или потенциально способных привести к расшифровке пользователя.

Отличается и способ получения наркотиков конечным наркопотребителем. В постсоветских странах пользователи забирают наркотики из тайников, куда их помещают специально подобранные организатором лица («минеры»), которые в случае задержания могут вывести на него. В то же время во многих зарубежных странах для доставки наркотиков задействованы обычные почтовые и курьерские службы доставки, которые используются «вслепую», не зная о том, что в почтовом отправлении находятся наркотики, не поддерживают никаких личных контактов с отправителем и по этой причине не могут использоваться полицией для изобличения преступника.

В отечественных интернет-магазинах для расчетов используются безналичные или электронные деньги. Поскольку для открытия счета или электронного кошелька требуется проведение идентификации их владельца, а информация о совершенных транзакциях и сопутствующие этому сведения сохраняются в банках, это дает правоохранительным органам доступ к значительному объему информации об обстоятельствах получения денег, уплаченных за

наркотики, об их дальнейшем движении, расходовании, о сопутствующих или идентифицирующих пользователя кошелька платежах, что в конечном счете позволяет получить информацию о преступниках, их соучастниках и об обстоятельствах совершения ими преступлений. Использование подставного лица, на которое оформляются счета и кошельки, лишь частично обеспечивает анонимность их реальных пользователей. В других странах мира при расчетах преступниками используется криптовалюта, специально созданная для того, чтобы обеспечивать анонимность сторон сделки при доступности информации о каждой транзакции. Перечисляя особенности ее использования, затрудняющие идентификацию владельца, отметим, что для открытия кошелька не требуется прохождение идентификации; криптовалюта циркулирует в теневом сегменте сети Интернет и может использоваться там же для приобретения товаров или услуг; несмотря на наличие общего доступа к перечню транзакций, цель перевода средств известна лишь сторонам сделки, идентификация которых с использованием этих данных сложна, как и установление их IP-адресов; для совершения операции не требуется третья сторона в виде банка или процессингового центра.

Принимая во внимание все более частое заимствование преступниками вышеперечисленных зарубежных «новаций» ведения преступной деятельности, становится очевидно, что правоохранительные органы Республики Беларусь в ближайшее время столкнутся со значительными сложностями в изобличении наркопреступников. В этой связи представляется актуальным сформулировать ряд перспективных направлений, которые могли бы существенно расширить тактические возможности оперативных подразделений по противодействию наркопреступности в сети Интернет.

Полагаем необходимым нормативно закрепить право правоохранительных органов на проведение в особых случаях удаленного обследования средств компьютерной техники, в том числе с использованием имеющихся недокументированных уязвимостей используемого преступниками программного обеспечения. К примеру, право на проведение подобных действий, по аналогии с традиционным обыском называемых «онлайновым обыском», имеет полиция Германии [1, с. 124–138].

Для обеспечения проведения указанных удаленных обследований необходимо предусмотреть возможность использования правоохранительными органами специализированного программного обеспечения, позволяющего осуществлять удаленный контроль за средствами компьютерной техники, используемыми для совершения преступлений, доступ к хранящимся на них данным и используемым удаленным сервисам (например, облачным ресурсам), а также дающего возможность отслеживать активность преступника в сети Интернет. Подобные меры, получившие неофициальное наименование «полицейский троян» уже давно предусмотрены в законодательстве и используются в практике деятельности полиции ряда государств мира [1, с. 130–134].

Список основных источников

1. Харевич, Д. Л. Негласное расследование в Германии : монография / Д. Л. Харевич ; М-во внутр. дел Респ. Беларусь, Акад. МВД. — Минск : Акад. МВД, 2010. — 287 с.

УДК 343.85(477)

А. В. Форос
профессор кафедры кибербезопасности
и информационного обеспечения
Одесского государственного университета внутренних дел,
кандидат юридических наук, доцент (Украина)

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УКРАИНЕ

Проблема компьютерной преступности привлекла внимание сотрудников правоохранительных органов зарубежных стран с момента широкого внедрения компьютерных технологий, что вызвало целый ряд негативных последствий и обострение ситуации в сфере защиты информации и информационных технологий. Анализ международной практики свидетельствует о том, что за последние тридцать лет в числе выявленных корыстных преступлений широкое распространение получили именно компьютерные преступле-